How to Use a DNS Archive to Improve Website Traffic, Reputation, and Performance

Posted on March 18, 2020

Infosec professionals are invariably responsible for guaranteeing that their organizations' websites remain accessible at all times. And so, they should be aware of the consequences of a single website outage. Network downtimes can cost most enterprises between $101,000 and $5,000,000 an hour.

The problem with outages, however, is that they mostly go undetected before they inflict noticeable damage. Customers don't usually report website issues such as page time-outs unless a purchase was involved. As such, the discovery of these glitches often comes too late since your search engine rankings or conversion rates have already dropped significantly. Worse still, malicious actors may have even taken over your site infrastructure.

So what can be done? Fortunately, these issues are preventable by ensuring that a website's Domain Name System (DNS) record values are correct with the aid of a DNS archive like Domain Database Download. For that reason, this article lists some possible ways of how a DNS Database can help with following your website maintenance best practices.

Website Maintenance Basics

Quality assurance should go beyond design and function. After all, what's the use of an eye-catching website if its page load time can't fit in with industry benchmarks. A study found that a site's mobile version should load at least within three seconds and, even then, bounce rates can still remain very high.

With the vast number of resources most corporate websites have to pull up, it's virtually impossible to bring down a site's load time substantially. Transactional websites are even more complicated. There are, however, some basic practices that can help boost a site's indexability, performance and views. That said, any website checkup should include the following:

Monitor your site for weaknesses

It usually takes more than 205 days to discover an intrusion. As a countermeasure, therefore, keep an eye out for unusual behaviors, such as severe website latency and the presence of lots of spam emails in your mail queue manager. Source code scanners can come in handy to check for malware signatures or patterns. You can also consult a **DNS archive** to see if all of your websites' DNS settings are correct or if the dates they were last updated match those in the maintenance records. As an additional important measure, you can also run domains in Domain Reputation API to check for any inherent weakness including the presence on a blacklist, SSL vulnerabilities, and more.

Watch out for broken links and redirects

Broken links and too many website redirects can impact your search engine optimization (SEO) score as well. Conduct a technical SEO audit and look into your internal linking scheme, site maps, and redirects with a website crawler to identify pages that may contain malicious links. You can also check when your host settings were last updated and if the IP records associated with them are clean aided by a **DNS archive**.

How a DNS Archive Can Boost Your Site Metrics

DNS archive data like DNS Database Download comes in CSV files so you can process them directly or import them to your favorite database system such as MySQL, Solr, etc. Such a resource can provide you with all your hostnames and the IP addresses they point to, which, in turn, can help you identify potential risks surrounding your web assets. Below are ways by which a DNS archive can help ensure your site metrics remain in the pink of health.

Prevents bad actors from compromising sites

An attacker can quickly compromise dangling subdomains for their gains. If you recently changed domains after a corporate rebrand, make sure you don't leave your old domain open to attacks. A connected compromised domain can land on a blacklist, which effectively reduces page views even for your new site. You can use a **DNS archive** to identify domains that you may have forgotten about. Delete these from your infrastructure so crafty hackers can't inject them with malware that can affect all assets sharing their hosts.

Validate name server (NS) records

Misaligned records could result in website downtime and potentially dangerous redirects. These may affect your site visitors' user experience and reputation score. A DNS database matches each domain to an IP address. Gather the relevant information from such a repository and run each through a name server check to make sure no one has tampered with your assets' settings.

Ensure that your sites do not share hosts with malicious pages

Sharing an IP address with a nefarious actor could result in blacklisting, thus preventing your site from being indexed and seen by your target audience. Being flagged by Google and other search engines is bound to hurt your bottom line. You can search for your IP addresses in a DNS database to learn more about the domains they host. Conduct in-depth investigations on them with domain research and monitoring tools. And if any of them prove malicious, you can ask your Internet service provider (ISP) for a different IP address.

Putting up a website does not end when it goes live. All site owners want their pages to live on. And with reliable DNS intelligence gleaned from a **DNS archive**, that is possible. Information sources like DNS Database can help identify exposed domain records to reduce risks of outages,

and most importantly, cyber attacks.